SPYWOLF

Security Audit Report

(TESTNET)

Completed on

March 21, 2022

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

OVERVIEW

This audit has been prepared for **GRAMZ** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

> *The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal*
>
> - SPYWOLF Team -

TABLE OF CONTENTS

CONTRACT INFO

Token Name
GRAMZ

Symbol
GRAMZ

Contract Address
0x795c7d1DA586F533799059D8b9a811Db1acCB93d

Network
Binance Smart Chain

Language
Solidity

Deployment Date
March 20, 2023

Verified?
Yes

Total Supply
777

Status
Not launched

TAXES

Buy Tax
50%

Sell Tax
25%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

CURRENT STATS

(As of March 21, 2023)

Liquidity

Not added yet

Burn

No burnt tokens

Status:

Not Launched!

MaxTxAmount

1

DEX

PancakeSwap

LP Address(es)

Liquidity not added yet

TOKEN TRANSFERS STATS

Transfer Count	2
Uniq Senders	2
Uniq Receivers	2
Total Amount	1554 GRAMZ
Median Transfer Amount	777 GRAMZ
Average Transfer Amount	777 GRAMZ
First transfer date	2023-03-20
Last transfer date	2023-03-20
Days token transferred	1

SMART CONTRACT STATS

Calls Count	6
External calls	6
Internal calls	0
Transactions count	6
Uniq Callers	1
Days contract called	1
Last transaction time	2023-03-20 18:36:22 UTC
Created	2023-03-20 18:30:13 UTC
Create TX	0xc19a66e859f1b9879426217a13265063c78d347b00468593f71fcf1e8b903df0
Creator	0xf8e832d40feead8c342271277480f75b2194a5f8

FEATURED WALLETS

Owner address	0xd09ae3ea459c5b3daec7f46e6ef2e6f6a662d2eb
Marketing fee receiver	0x52974beF278A71C14F612dA101ad1bA2Ce634241
Ecosystem fee receiver	0x18BA76A1e8bD204c56242b5209F723c3bc318172
Dev fee receiver	0xc868e5F599f39AF9D2b53425dEe994553582a96e
LP address	**Liquidity not added yet**

TOP 3 UNLOCKED WALLETS

1 100% Same as owner

2 N/A

3 N/A

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

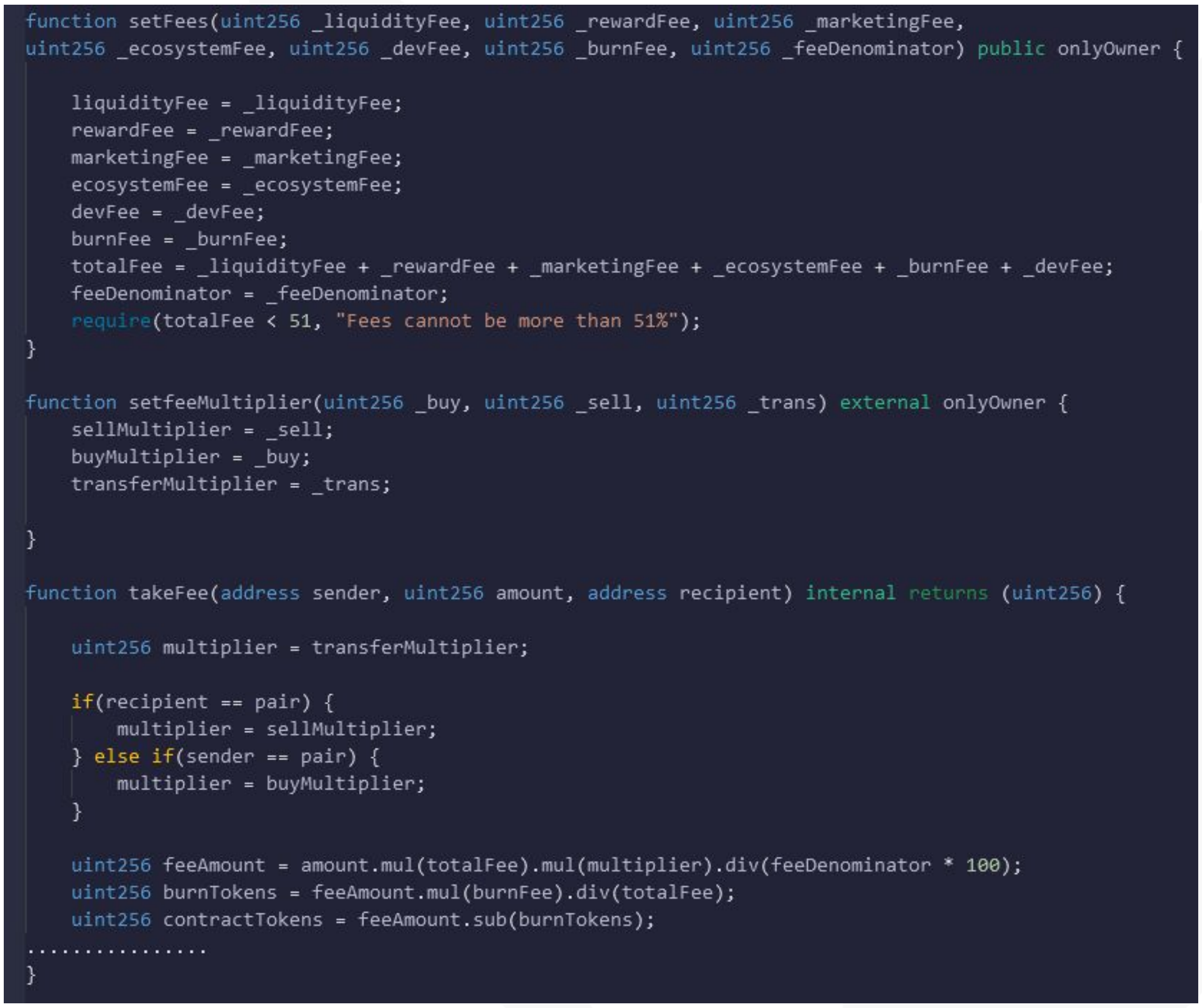
Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

Owner can set buy/sell fees up to 100%.
When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make.



```
function setFees(uint256 _liquidityFee, uint256 _rewardFee, uint256 _marketingFee,
uint256 _ecosystemFee, uint256 _devFee, uint256 _burnFee, uint256 _feeDenominator) public onlyOwner {

    liquidityFee = _liquidityFee;
    rewardFee = _rewardFee;
    marketingFee = _marketingFee;
    ecosystemFee = _ecosystemFee;
    devFee = _devFee;
    burnFee = _burnFee;
    totalFee = _liquidityFee + _rewardFee + _marketingFee + _ecosystemFee + _burnFee + _devFee;
    feeDenominator = _feeDenominator;
    require(totalFee < 51, "Fees cannot be more than 51%");
}

function setfeeMultiplier(uint256 _buy, uint256 _sell, uint256 _trans) external onlyOwner {
    sellMultiplier = _sell;
    buyMultiplier = _buy;
    transferMultiplier = _trans;

}

function takeFee(address sender, uint256 amount, address recipient) internal returns (uint256) {

    uint256 multiplier = transferMultiplier;

    if(recipient == pair) {
        multiplier = sellMultiplier;
    } else if(sender == pair) {
        multiplier = buyMultiplier;
    }

    uint256 feeAmount = amount.mul(totalFee).mul(multiplier).div(feeDenominator * 100);
    uint256 burnTokens = feeAmount.mul(burnFee).div(totalFee);
    uint256 contractTokens = feeAmount.sub(burnTokens);
...............
}
```

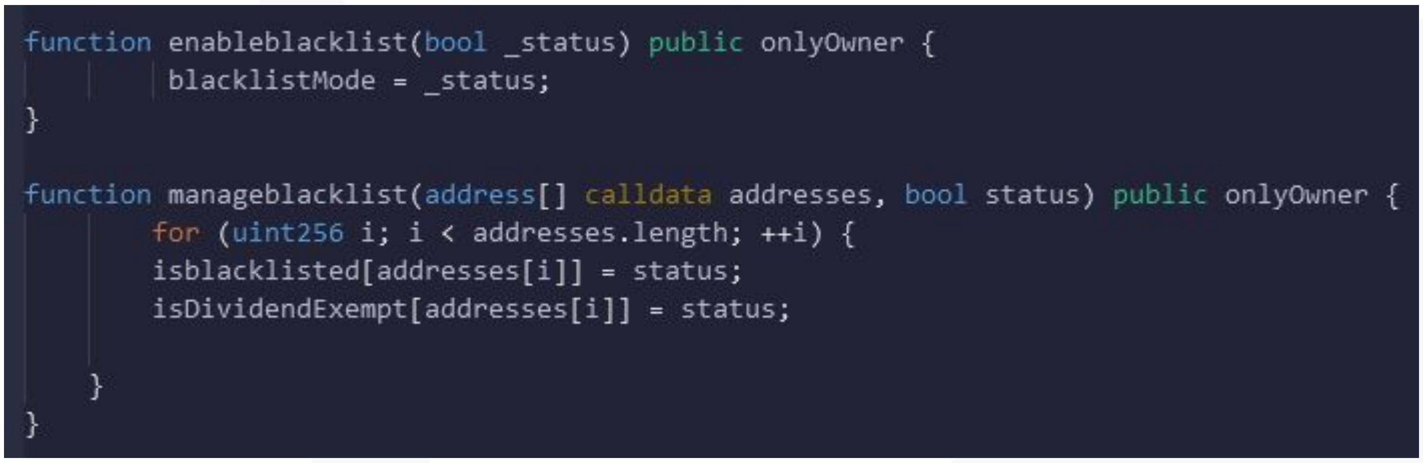
Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

- Recommendation:
    - Considered as good tax deduction practice is buy and sell fees combined not to exceed 25%.

FOUND THREATS

⚠ High Risk

Owner can blacklist address.
For blacklisted address it is forbidden to transfer/sell tokens.



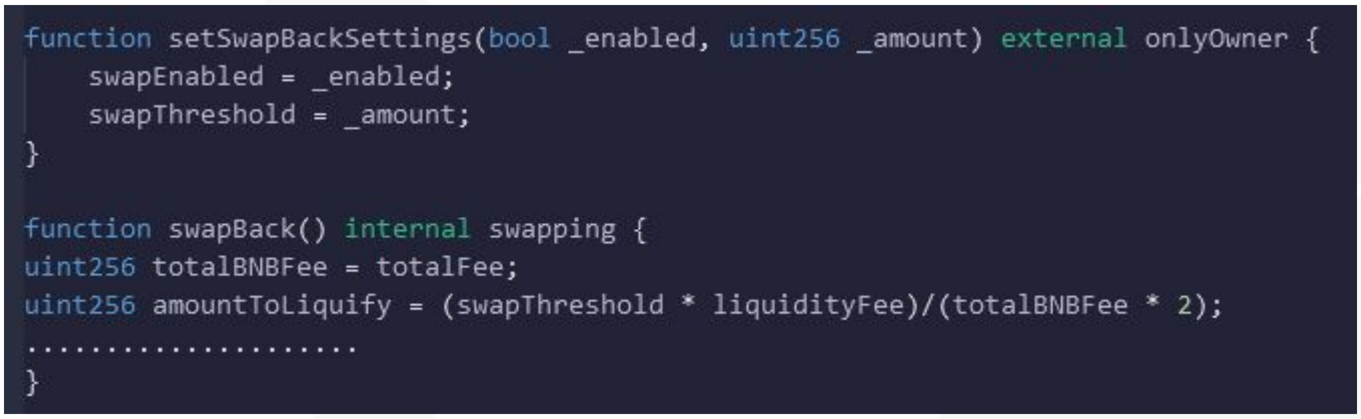
```
function enableblacklist(bool _status) public onlyOwner {
        blacklistMode = _status;
}

function manageblacklist(address[] calldata addresses, bool status) public onlyOwner {
        for (uint256 i; i < addresses.length; ++i) {
        isblacklisted[addresses[i]] = status;
        isDividendExempt[addresses[i]] = status;

    }
}
```

- Recommendation:
  - Considered as good practice is to implement automated protection to avoid snipe bots and front running bots instead of manual blacklisting.

FOUND THREATS

⚠ High Risk

Owner can change autoSwap settings.
If the swapThreshold variable is set to 0 or very low number, contract will halt and selling will fail.



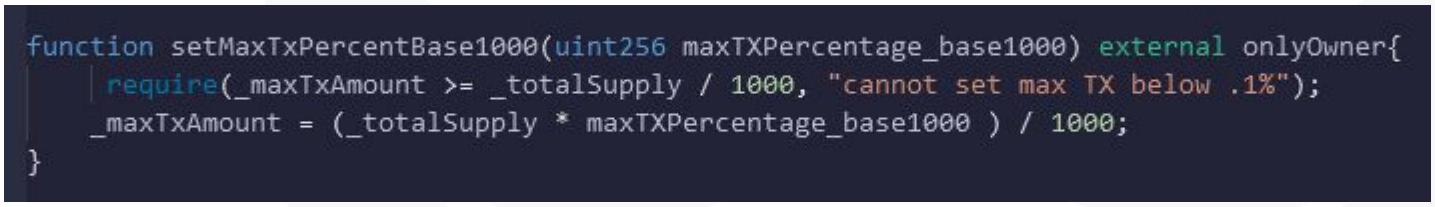
```
function setSwapBackSettings(bool _enabled, uint256 _amount) external onlyOwner {
    swapEnabled = _enabled;
    swapThreshold = _amount;
}

function swapBack() internal swapping {
uint256 totalBNBFee = totalFee;
uint256 amountToLiquify = (swapThreshold * liquidityFee)/(totalBNBFee * 2);
.....................
}
```

- Recommendation:
  - Ensure that the *swapThrehold* variable is always above 1 token (consider decimals).

FOUND THREATS

⚠ High Risk

Owner can set max transaction limit without limitation.
If maxTXPercentage_base1000 is set to 0 it will effectively set max transaction limit to 0, making it impossible for any further buy/sells.



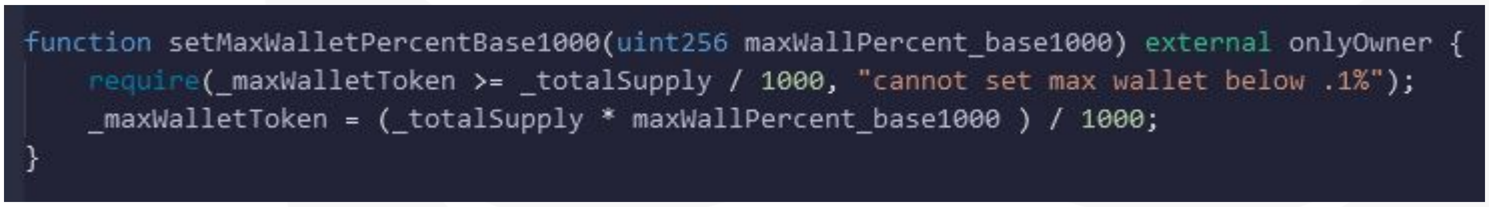
```
function setMaxTxPercentBase1000(uint256 maxTXPercentage_base1000) external onlyOwner{
    require(_maxTxAmount >= _totalSupply / 1000, "cannot set max TX below .1%");
    _maxTxAmount = (_totalSupply * maxTXPercentage_base1000 ) / 1000;
}
```

- Recommendation:
  - Ensure that *maxTXPercentage_base1000* variable is checked instead of *_maxTxAmount* variable.

FOUND THREATS

⚠ High Risk

Owner can set max wallet below 0.1% of total supply.
If set to very low number this can forbid new buyers from buying large amount of tokens with single wallet.



```
function setMaxWalletPercentBase1000(uint256 maxWallPercent_base1000) external onlyOwner {
    require(_maxWalletToken >= _totalSupply / 1000, "cannot set max wallet below .1%");
    _maxWalletToken = (_totalSupply * maxWallPercent_base1000 ) / 1000;
}
```

- Recommendation:
  - Ensure that *maxWallPercent_base1000* variable is checked instead of *_maxWalletToken* variable.

FOUND THREATS

⚠ Medium Risk

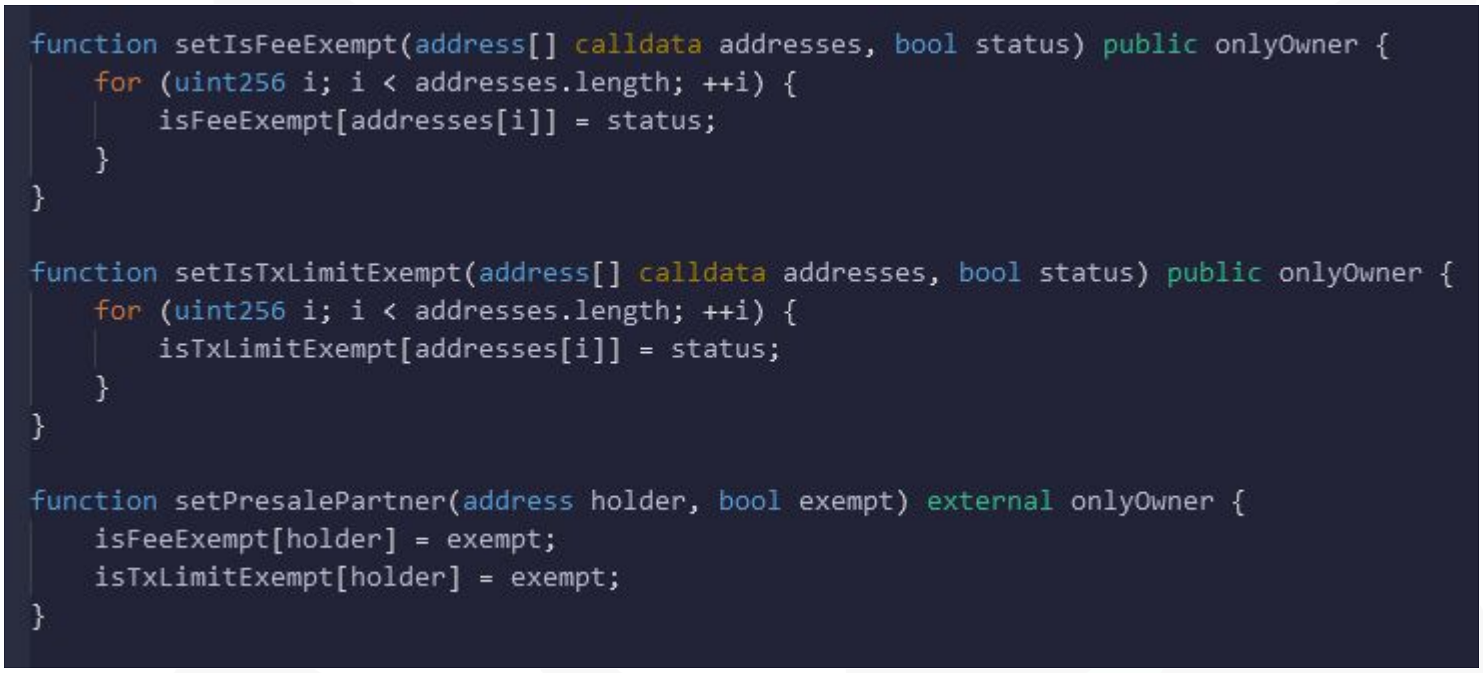
No medium risk-level threats found in this contract.

⚠ Low Risk

No low risk-level threats found in this contract.

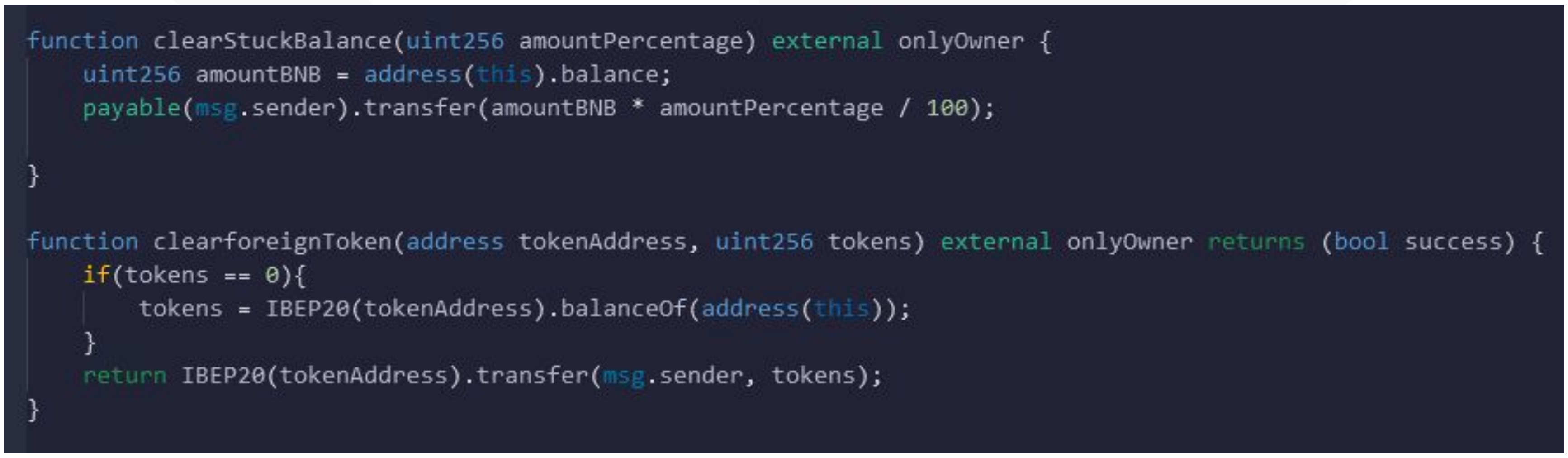
Informational

Owner can exclude address from fees and max transaction limits.
When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.
When address is excluded from max transaction limits, such limits (if present) wont apply for it.



```
function setIsFeeExempt(address[] calldata addresses, bool status) public onlyOwner {
    for (uint256 i; i < addresses.length; ++i) {
        isFeeExempt[addresses[i]] = status;
    }
}

function setIsTxLimitExempt(address[] calldata addresses, bool status) public onlyOwner {
    for (uint256 i; i < addresses.length; ++i) {
        isTxLimitExempt[addresses[i]] = status;
    }
}

function setPresalePartner(address holder, bool exempt) external onlyOwner {
    isFeeExempt[holder] = exempt;
    isTxLimitExempt[holder] = exempt;
}
```

Owner can withdraw any tokens from the contract
When this function is present, in cases tokens sent into the contract by mistake or purposefully, contract's owner can retrieve them.



```
function clearStuckBalance(uint256 amountPercentage) external onlyOwner {
    uint256 amountBNB = address(this).balance;
    payable(msg.sender).transfer(amountBNB * amountPercentage / 100);

}

function clearforeignToken(address tokenAddress, uint256 tokens) external onlyOwner returns (bool success) {
    if(tokens == 0){
        tokens = IBEP20(tokenAddress).balanceOf(address(this));
    }
    return IBEP20(tokenAddress).transfer(msg.sender, tokens);
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1 Consider fundamental tradeoffs

2 Be attentive to blockchain properties

3 Ensure careful rollouts

4 Keep contracts simple

5 Stay up to date and track development

GRAMZ

GOOD PRACTICES FOUND

✓ The owner cannot mint new tokens after deployment

✓ The smart contract utilizes "SafeMath" to prevent overflows

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ **OVER 150 SUCCESSFUL CLIENTS**
- ✓ **MORE THAN 500 SCAMS EXPOSED**
- ✓ **MILLIONS SAVED IN POTENTIAL FRAUD**
- ✓ **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- ✓ **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

SPYWOLF.NETWORK

@SPYWOLFNETWORK

@SPYWOLFOFFICIAL

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.